IN THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the Application:

LISTING OF CLAIMS:

Claims 1-36 (Canceled).

37. (Previously Presented) An apparatus to support surveillance, the apparatus comprising:

a camera to generate a video signal that varies depending on sensed images;

a memory device to store at least first and second encryption keys;

means for encrypting the video signal using the first encryption key and means for encrypting the first encryption key with the second encryption key to produce an output signal including at least the encrypted video signal and the encrypted first encryption key; and

means for identifying objects associated with the sensed images and embedding encrypted data information identifying the recognized object in the output signal;

wherein the means for embedding encrypted data information identifying the recognized object in the output signal includes means for:

encrypting data identifying objects associated with the sensed images with a third key, the third key being distinct from the first key so that a user, possessing only the third key but not the first key, can decrypt the data identifying objects without having the capability to decrypt the video signal; and

including the data encrypted with the third key in the output signal; and

wherein the means for identifying objects associated with the sensed images includes means for analyzing one sensed image of the sensed images to identify a person associated with a pattern depicted in the one sensed image.

38. (Previously Presented) A computer program product including a computer-readable medium having instructions stored thereon for processing data information, such that the instructions, when carried out by a processing device, cause the processing device to perform the steps of:

receiving a video signal that varies depending on sensed images;

encrypting the video signal using a first key;

encrypting the first key using a second key, the first and second key being different than each other;

including at least the encrypted first key and encrypted video signal in the output signal;

identifying objects associated with the sensed images; and

embedding encrypted data information identifying the recognized object in the output signal;

wherein the step of embedding encrypted data information identifying the recognized object in the output signal includes:

encrypting data identifying objects associated with the sensed images with a third key, the third key being distinct from the first key so that a user, possessing only the third key but not the first key, can decrypt the data identifying objects without having the capability to decrypt the video signal; and

including the data encrypted with the third key in the output signal; and

wherein the step of identifying objects associated with the sensed images includes analyzing one sensed image of the sensed images to

identify a person associated with a pattern depicted in the one sensed image.

Claims 39-42 (Canceled).

43. (Previously Presented) A method for generating an output signal from a video data acquisition system, the method comprising:

receiving a video signal that varies depending on sensed images;

encrypting the video signal using a first key;

encrypting the first key using a second key;

including at least the encrypted first key and encrypted video signal in the output signal;

implementing a recognition algorithm to identify objects associated with the sensed images;

in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal; and

randomly generating a new encryption key for encrypting different portions of the video signal over time;

wherein implementing the recognition algorithm to identify objects associated with the sensed images includes:

analyzing one sensed image of the sensed images to identify a person associated with a pattern depicted in the one sensed image.

44. (Previously Presented) A method as in claim 43 wherein embedding encrypted data information identifying the recognized object in the output signal includes:

encrypting data identifying objects associated with the sensed images with a third key, the third key being distinct from the first key so that a user, possessing only the third key but not the first key, can decrypt

the data identifying objects without having the capability to decrypt the video signal; and

including the data encrypted with the third key in the output signal.

45. (Previously Presented) An apparatus to support surveillance, the apparatus comprising:

a camera to generate a video signal that varies depending on sensed images;

a memory device to store at least first and second encryption keys;

a processor that encrypts the video signal using the first encryption key, the processor encrypting the first encryption key with the second encryption key, the processor producing an output signal including at least the encrypted video signal and the encrypted first encryption key;

a recognition system to identify objects associated with the sensed images, the processor embedding encrypted data information identifying the recognized object in the output signal; and

an encryption key generator that randomly generates a new value for the first encryption key to uniquely encrypt different portions of the video signal over time;

wherein the recognition system analyzes one sensed image of the sensed images to identify a person associated with a pattern depicted in the one sensed image.

46. (Previously Presented) An apparatus as in claim 45 wherein the processor, when embedding encrypted data information identifying the recognized object in the output signal:

encrypts data identifying objects associated with the sensed images with a third key, the third key being distinct from the first key so that a user, possessing only the third key but not the first key, can decrypt

the data identifying objects without having the capability to decrypt the video signal; and

includes the data encrypted with the third key in the output signal.

47. (Previously Presented) An apparatus as in claim 37 wherein the apparatus further comprises:

means for randomly generating a new encryption key for encrypting different portions of the video signal over time.

Claim 48 (Canceled).

49. (Previously Presented) A computer program product as in claim 38 wherein the instructions, when carried out by the processing device, cause the processing device to further perform the step of:

randomly generating a new encryption key for encrypting different portions of the video signal over time.

Claims 50-51 (Canceled).

52. (Previously Presented) A method for generating an output signal from a video data acquisition system, the method comprising:

receiving a video signal that varies depending on sensed images;

encrypting the video signal using a first key;

encrypting the first key using a second key;

including at least the encrypted first key and encrypted video signal in the output signal;

implementing a recognition algorithm to identify objects associated with the sensed images; and

in response to recognizing an object, embedding encrypted data identifying the recognized object in the output signal;

wherein embedding encrypted data identifying the recognized object in the output signal includes:

encrypting data identifying objects associated with the sensed images with a third key, the third key being distinct from the first key so that a user, possessing only the third key but not the first key, can decrypt the data identifying objects without having the capability to decrypt the video signal; and

including the data encrypted with the third key in the output signal; and

wherein implementing the recognition algorithm to identify objects associated with the sensed images includes:

analyzing one sensed image of the sensed images to identify a person associated with a pattern depicted in the one sensed image.

53. (New) A method of conducting surveillance comprising:

placing a video data acquisition system (VDAS) in a public place to conduct surveillance of the public place;

operating the VDAS, the VDAS producing a video signal depicting the public place, the video signal including a series of frames that correspond to different moments in time;

encrypting the video signal using a first key, the first key being randomly generated such that a new randomly generated first key is used at different points in time;

encrypting the first key using a second key;

including at least the encrypted first key and encrypted video signal in an output signal;

operating an image analyzer, the image analyzer:

receiving the video signal from the VDAS;

identifying a person depicted in a frame of the video signal by analyzing each frame of the video signal to look for patterns corresponding to specific persons; and

for every identified person, embedding a code corresponding to that identified person in the output signal, the code being associated with the particular frame in which the pattern corresponding to the identified person was found;

storing the output signal in a data storage medium;

searching the data storage medium for a code corresponding to a specific person; and

upon finding the code corresponding to the specific person in the data storage medium:

decrypting, with the second key, the first key used to encrypt a portion of the video signal containing the frames associated with the code corresponding to the specific person;

decrypting, with the decrypted first key, the portion of the video signal containing the frames associated with the code corresponding to the specific person; and

displaying the portion of the video signal containing the frames associated with the code corresponding to the specific person.

54. (New) A method as in claim 53 wherein embedding the code corresponding to that identified person in the output signal includes:

encrypting the code with a third key, the third key being distinct from the first key so that a user, possessing only the third key but not the first key, can decrypt the code without having the capability to decrypt the video signal; and

including the data encrypted with the third key in the output signal.